U.S. House of Representatives
Committee on Transportation and Infrastructure
Washington, DC 20515

James L. Oberstar
Chairman

John L. Mica
Ranking Republican Member

David Heymsfeld, Chief of Staff
Ward W. McCarragher, Chief Counsel

James W. Coon II, Republican Chief of Staff

January 22, 2008

SUMMARY OF SUBJECT MATTER

TO: Members of the Subcommittee on Coast Guard and Maritime Transportation

FROM: Subcommittee on Coast Guard and Maritime Transportation Staff

SUBJECT: Follow-up Hearing on Transportation Worker Identification Credential

PURPOSE OF THE HEARING

On Wednesday, January 23, 2008, at 2:00 p.m., in Room 2167 Rayburn House Office Building, the Subcommittee on Coast Guard and Maritime Transportation will meet to examine the roll-out of the Transportation Worker Identification Credential ("TWIC"). Active enrollment has been underway for approximately 90 days.

CREATION OF TWIC-BASED ACCESS CONTROL PROGRAM

Section 70105 of Title 46 of the United States Code (46 U.S.C. 70105) requires the Department of Homeland Security ("DHS") to issue a biometric credential to ensure that workers who pose a risk to the national security of the United States do not have unescorted access to the secure areas of sensitive maritime facilities, including ports and vessels.

According to Section 70105, anyone who needs unescorted access to secure areas of vessels, ports, and other transportation facilities is required to obtain a TWIC. Such individuals include, but are not limited to, port facility employees, longshoremen, truck drivers, contractors, and any others who may require unescorted access to the secure areas of a facility or vessel as part of their work responsibilities. In addition, all individuals who hold merchant mariner credentials issued by the United States Coast Guard are also required to obtain TWIC cards.

The Coast Guard and the Transportation Security Administration ("TSA") have issued regulations that require vessel owners/operators to begin controlling access to secure areas of vessels through use of the TWIC by September 25, 2008. The Coast Guard has not yet announced

when shore-based facilities will be required to utilize TWICs to control access to secure areas, though compliance is expected to be phased in by Coast Guard "Captain of the Port" zones beginning with high volume port areas.

IMPLEMENTATION OF THE TWIC-BASED SECURITY SYSTEM

TSA is responsible for the issuance of TWIC cards to individuals. As part of this process, TSA conducts background checks on enrollees and produces the physical TWIC cards. TSA also handles requests for waivers from those individuals who initially have been disqualified from receiving a TWIC.

TSA has contracted with Lockheed Martin to manage the enrollment process. The contract awarded by TSA to Lockheed covers an initial 15-month period and provides four options that allow the contract to be extended through a total of five years.

Under the contract, Lockheed is responsible for operating enrollment facilities. Lockheed personnel staff the enrollment centers and collect enrollment data from TWIC applicants. This data is then submitted to TSA, which conducts the required background checks on the applicant and produces the TWIC cards for approved applicants. Completed TWICs are then shipped to Lockheed, which distributes the cards through the enrollment centers it operates. Lockheed and its corporate partners are also responsible for conducting all outreach activities to inform workers in the maritime industry of the implementation of the TWIC program and of how TWIC cards can be obtained from enrollment centers.

The United States Coast Guard is responsible for enforcing the use of the TWIC card to control access to secure parts of transportation facilities and vessels. The Coast Guard's responsibilities include publishing the final rule that will guide the installation of the card readers that will be used to read TWICs for access control purposes and then enforcing the proper use of card readers. The Coast Guard is also responsible for reviewing and enforcing vessel and facility security plans (through which secure areas are designated).

The TWIC program is not meant to replace any access control measures that individual facilities put in place. Individual transportation facilities can incorporate the TWIC card into their existing physical access control systems.

ESCORTING/MONITORING

Facilities and vessel owners/operators are required to exercise responsibility for controlling access to secure (and restricted) areas of their property, including ensuring that non-TWIC holders who enter secure and restricted areas (restricted areas are areas within secure areas that have additional entrance requirements because they may present a heightened opportunity for a transportation security incident) are escorted by TWIC holders and that non-TWIC holders who enter areas that are secure but not restricted are at least monitored by TWIC holders. Monitoring can be accomplished by close-circuit television, security patrols or automatic intrusion detection devices. If non-TWIC holders are being monitored, the monitoring process must enable sufficient

observation of the non-TWIC holder to ensure that the facility owner/operator can respond quickly if the non-TWIC holder enters an unauthorized area or engages in unauthorized activities.

ELIGIBILITY FOR A TWIC

U.S. nationals are eligible to hold TWICs, as are certain non-U.S. citizens who are lawfully present in the United States. Non-U.S. citizens who may hold TWICs include, but are not limited to, those individuals who are lawful permanent residents and individuals who hold any of a variety of work-related visas that make a non-U.S. citizen eligible to work in the U.S. maritime industry.

The SAFE Port Act of 2006 required DHS to permanently disqualify any individual convicted of treason, espionage, sedition, or terrorism from ever receiving a TWIC. This list was amended last year in the Implementing Recommendations of the 9/11 Commission Act of 2007, which enacted a set of crimes that constitute "permanent disqualifying criminal offenses" and a set of crimes that constitute "interim disqualifying felonies."

Permanent Disqualifying Crimes

Those who are convicted of the following crimes – or who are found not guilty of these crimes by reason of insanity – are permanently disqualified from receiving a TWIC:

- Espionage, or conspiracy to commit espionage.
- Sedition, or conspiracy to commit sedition.
- Treason, or conspiracy to commit treason.
- A federal or state crime of terrorism, or conspiracy to commit such a crime.
- A crime involving a transportation security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. (Work stoppage, or other nonviolent employee-related action resulting from an employer-employee dispute is not considered to be a transportation security incident.)
- Improper transportation of a hazardous material as defined in federal or State law.
- Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device, as defined by federal regulation.
- Murder.
- Making a threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportation system, or an infrastructure facility.
- Violations of the Racketeer Influenced and Corrupt Organizations Act or any comparable state law, where one of the predicate acts found by a jury or admitted by the defendant consists of one of the crimes listed above.
- Attempt to commit espionage, sedition, treason, or terrorism.
- Conspiracy or attempt to commit the remainder of the crimes above.

Interim Disqualifying Felonies

If an applicant is convicted of any of the following crimes – or is found not guilty of any of these crimes by reason of insanity – within seven years of the date of their application for a TWIC, or if the applicant was released from incarceration for one of these crimes within five years of the date of his or her application for a TWIC, the applicant is disqualified from receiving a TWIC for the specified interim period. The crimes are:

- Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipment, transportation, delivery, import, export of, or dealing in a firearm or other weapon, as defined by federal regulation.
- Extortion.
- Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering where money laundering is related to any of the list of permanently disqualifying crimes or interim disqualifying crimes. (Welfare fraud and the passing of bad checks do not constitute dishonesty, fraud, or misrepresentation of purposes of this paragraph.)
- Bribery.
- Smuggling.
- Immigration violations.
- Distribution of, possession with intent to distribute, or importation of a controlled substance.
- Arson.
- Kidnapping or hostage taking.
- Rape or aggravated sexual abuse.
- Assault with intent to kill.
- Robbery.
- Conspiracy or attempt to commit the crimes listed above.
- Violations of the Racketeer Influences and Corrupt Organizations Act, or comparable state law other than the violations listed in the previous paragraph, for fraudulent entry into secure seaport areas.

A person under warrant or indictment for any of the disqualifying crimes may also not hold a TWIC until the warrant is cleared or the indictment is dismissed.

THE TWIC CARD

The physical TWIC card is based on smart card technology. It contains an integrated circuit chip that provides biometric identification without requiring a connection to a central database. The card also provides room for the addition of future technology applications.

The TWIC card's chip can be read either by inserting the card into a slot in a card reader or by holding the card within 10 centimeters of a card reader that does not require physical contact with the card to verify the information on the card. Additionally, the card contains a magnetic stripe (such as is commonly found on credit cards) that can be swiped through a stripe reader and the card features a bar code that can be read by a bar code reader. TWICs will be used in card readers in

conjunction with PIN numbers which card holders select at the time of activation of the TWIC and which must be entered into the readers when the TWIC is used for access control purposes.

Before TWIC card readers are installed on vessels and at transportation facilities, access to secure areas will be controlled by visual inspection of TWIC cards. After card readers are in place at transportation facilities, TWICs will be scanned through the card readers. The final rulemaking explaining where such readers will be required to be installed (including the types of vessels that will be required to install them) has not yet been promulgated by the Coast Guard.

Importantly, possession of a TWIC does not bestow the right of entry into a secure area on the card holder. Access to a secure area is always controlled by the owner and/or operator of a vessel or facility.

THE TWIC ENROLLMENT PROCESS

An individual applies for a TWIC card at an enrollment center. According to TSA, a total of 147 permanent enrollment centers will eventually be opened in the United States. The enrollment centers are being opened on a rolling basis. The first enrollment center opened in Wilmington, Delaware, on October 16, 2007. As of January 11, 2008, 49 TWIC enrollment centers had been opened around the nation, and an additional 20 mobile enrollment centers had been established.

Mobile centers are enrollment stations that are set up in locations – such as at a maritime facility or in the office of a large maritime employer – that are not directly controlled by Lockheed. Mobile centers offer Lockheed the opportunity to enroll large populations concentrated in a single location.

Pursuant to section 520 of the Department of Homeland Security Appropriations Act, 2004 (P.L. 108-90), the recipients of the TWIC card must cover the full costs of the program. The cost of applying for a TWIC is $132.50. Enrollment for a person who has previously completed a criminal history check equivalent to that required for TWIC enrollment costs is $105.25. Equivalent checks include checks conducted prior to the issuance of a Hazardous Materials Endorsement, a Free and Secure Trade card, a Merchant Mariner Document issued after February 3, 2003, or a Merchant Marine License issued after January 13, 2006. The cost of replacing a lost or damaged card is $60.

The TWIC card is valid for five years from the date of issuance. Cards issued on the basis of security checks associated with other documents are valid for the five-year period from the date listed on the credential for which the comparable security threat assessment was conducted.

Original estimates had projected that approximately 750,000 individuals would need a TWIC card. DHS now indicates that the total population needing a TWIC may actually be as high as one million individuals. According to TSA, as of January 15, 2008, nearly 109,000 pre-enrollments had been initiated; 48,873 enrollments had been completed; 25,366 TWIC cards had been printed (as of January 14); and 11,795 cards had been picked up and activated. Average enrollment time was reported by Lockeed to be 10.61 minutes, but there have been reports from applicants of wait times ranging from two to five hours.

Those applying for a TWIC are able to complete a pre-enrollment process over the Internet. Through that process, the applicant submits his/her personal information and then makes an appointment to come to an enrollment center where he/she completes the enrollment process. Applicants may also walk in to an enrollment center without completing the pre-enrollment process on-line but they will have to wait in line for a turn. Pre-enrolling is estimated to save an applicant 10 minutes at the enrollment center.

At the enrollment center, applicants submit a 10-digit fingerprint scan and provide identity verification documents; a digital photograph is also taken. This information is submitted by Lockheed to TSA. TSA conducts a fingerprint-based criminal background check on all TWIC applicants; TSA also checks applicants against terrorism watch lists and databases and performs an immigration status check.

Lockheed reports that the fingerprint rejection rate (due to poor print quality) among TWIC applicants is approximately two percent. Currently, individuals whose fingerprints are rejected must return to an enrollment center to submit a second set of fingerprints. The FBI, which conducts the actual fingerprint-based criminal background check, requires that fingerprints be submitted for consideration twice. If, after two attempts, the FBI cannot read a set of fingerprints, the individual's name will be submitted for a name-based criminal background check. Although not currently available, Lockheed reports that it is working to automatically capture two sets of fingerprints at the time of enrollment.

After an applicant's security assessment has been completed and if he or she is approved to receive a TWIC, he or she will be notified that his or her TWIC is available for pick-up at the same center in which he or she enrolled. During the pick-up process, the applicant's identity is again verified through a fingerprint recognition system. The applicant's card will be activated after the applicant has selected and stored on the card a 6-digit PIN number (which is used with the TWIC in TWIC readers).

Significant delays have been encountered by some individuals visiting enrollment centers to pick up and activate TWICs. Lockheed reports that it is planning to reduce such delays by enabling individuals to make pick up/activation appointments in the same way that individuals who pre-enroll for a TWIC can make an appointment to complete the enrollment process. Lockheed has indicated that pick-up appointments may begin to be available in early February.

WAIVERS FOR DISQUALIFYING OFFENSES

TSA can reject an application for a TWIC for past criminal history or for determination on any basis that the applicant poses a threat to the security of the United States. If the applicant feels that the assessment of threat is based on incorrect information, the applicant may file an appeal with the TSA. As part of the appeal, the applicant must provide proof that TSA's information is in error. As of January 13, 2008, 817 individuals had been sent initial disqualification letters, 270 appeals had been requested, and 216 appeals had been granted.

If the applicant does not dispute information used by TSA to disqualify him or her from holding a TWIC, but wishes to argue that he or she is not a threat to the security of a transportation facility, he/she can seek a waiver from TSA. An individual seeking a waiver in response to the

TSA's determination that he or she is not qualified to hold a TWIC must provide all information needed to support their waiver requests within 60 days from the time they receive notice that his or her application for a TWIC was rejected.

If an applicant knows that there is something in his or her background that may disqualify him or her from receiving a TWIC, the applicant can also file a request for a waiver at the time he or she submits his or her initial application.

If TSA rejects a waiver request, the agency will issue a Final Determination of Threat Assessment, explaining why the agency has rejected the application for the waiver (and the TWIC application). An applicant may seek review of the Final Determination by an Administrative Law Judge ("ALJ") by requesting the review within 30 days of receiving TSA's Final Determination; requests for ALJ review can include requests for in-person hearings before the ALJ. These requests for reviews will be considered by the Coast Guard Administrative Law Judge system.

If an ALJ upholds TSA's Final Determination of Threat Assessment and the concomitant denial of the waiver request, the applicant can appeal that finding to the TSA Final Decision Maker. If the TSA Final Decision Maker denies that appeal, that decision is considered final agency action. The applicant can then appeal that decision to the Court of Appeals.

If the ALJ grants the waiver request, the TSA can agree with that decision and grant the waiver – or the TSA Final Decision Maker can reverse the ALJ decision by upholding the Final Determination of Threat Assessment. If the TSA Final Decision Maker reverses the ALJ decision and denies the waiver, the applicant may appeal that decision to the Court of Appeals.

TSA indicates that as of January 13, 2008, 10 waivers had been requested but no decisions had been reached by TSA on these waiver requests. As a result, no cases have been appealed to the ALJ system.

NEW HIRE WORK AUTHORITY

Individuals who are newly hired in the maritime industry are allowed to enter secure areas of a vessel or a transportation facility for 30 days if (1) they have applied for a TWIC; (2) they state in writing that they will not be applying for a waiver; (3) they have passed a name-based security check by TSA; and (4) they are monitored in secure areas by employees who hold a TWIC. Newly hired employees must use a government-issued ID to obtain admission to a secure area. Facilities and vessels are not allowed to have more than 25 percent of their workforce using this authority. Further, the new hire work authority does not apply to newly hired personnel who will have vessel/terminal security as their primary work responsibility.

REVOKED TWICS

Individuals who have been convicted of a disqualifying offense or who no longer meet applicable immigration standards are required to notify TSA of these situations and to relinquish their TWICs to their employer, TSA, or to an enrollment center.

TSA has created a "hot list" that lists all invalid TWICs (including TWICs that have been revoked or been reported missing). It is necessary for vessels and port facilities to check the "hot list" regularly to become aware of TWICs that are invalid and to ensure that such TWICs are prohibited from being used to gain unescorted access to secure areas of transportation facilities.

PREVIOUS COMMITTEE ACTION

The Subcommittee on Coast Guard and Maritime Transportation has held numerous hearings to review the TWIC program. Most recently, the Subcommittee held a hearing on the program on July 12, 2007. During that hearing, the Subcommittee received testimony from the Coast Guard and TSA regarding the planned roll-out of the TWIC and received testimony from a number of witnesses in the maritime industry who expressed concerns about how the TWIC roll-out process would proceed when it was initiated. The Subcommittee Chairman committed at that time to hold a follow-up hearing that would enable the Subcommittee to receive a status report on the roll-out of TWIC once enrollment had begun.

WITNESSES

PANEL I

Rear Admiral Brian Salerno
Assistant Commandant for Marine Safety, Security, and Stewardship
U.S. Coast Guard

Ms. Maurine Fanguy
TWIC Program Manager
Transportation Security Administration

PANEL II

Ms. Judy F. Marks
President
Lockheed Martin
Transportation and Security Solutions

The Honorable John Porcari
Secretary
Maryland Department of Transportation